Journal of Pure and Applied Algebra 220 (2016) 2828–2835

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Indivisibility of class numbers of real quadratic function fields

Jungyun Lee [a,**,1,3], Yoonjin Lee [b,*,2,3]

[a] *Institute of Mathematical Sciences, Ewha Womans University, 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 120-750, South Korea*
[b] *Department of Mathematics, Ewha Womans University, 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 120-750, South Korea*

ARTICLE INFO

Article history:
Received 15 September 2014
Received in revised form 26 January 2016
Available online 23 February 2016
Communicated by I.M. Duursma

MSC:
11R29; 11R58

ABSTRACT

In this paper we work on indivisibility of the class numbers of *real* quadratic function fields. We find an explicit expression for a lower bound of the density of real quadratic function fields (with constant field $\mathbb{F}$) whose class numbers are not divisible by a given prime ℓ. We point out that the explicit lower bound of such a density we found only depends on the prime ℓ, the degrees of the discriminants of real quadratic function fields, and the condition: either $|\mathbb{F}| \equiv 1 \pmod{\ell}$ or not.

1. Introduction

There have been active developments on divisibility or indivisibility of class numbers of quadratic fields, for instance [4,6,8–11,13–17]. Specially, in [4,16], indivisibility of class numbers of real quadratic number fields has been studied with a connection with *Greenberg conjecture*. Existence of real quadratic fields whose class numbers are not divisible by a given prime p is closely related to the existence of real quadratic fields whose cyclotomic $\mathbb{Z}_p$-extensions have the *Iwasawa λ-invariant* zero (which is Greenberg Conjecture). It is thus important to study the existence of real quadratic fields whose class numbers are not divisible by p. In [4], Byeon finds an infinite set S of real quadratic fields whose class numbers are not divisible by a given prime p; however, this set S has no positive density. According to Cohen–Lenstra heuristics, it is conjectured that the density of real quadratic fields whose class numbers are not divisible by a given prime p is positive; but, it is not proved yet.

* Corresponding author.
** Principal corresponding author.
E-mail addresses: lee9311@ewha.ac.kr (J. Lee), yoonjinl@ewha.ac.kr (Y. Lee).
[1] The first named author was also supported by the National Research Foundation of Korea (NRF) grant founded by the Korea government (2011-0023688).
[2] The second named author by the National Research Foundation of Korea (NRF) grant founded by the Korea government (MEST) (2014-002731).
[3] The authors were supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827).

http://dx.doi.org/10.1016/j.jpaa.2016.01.002
0022-4049/

On the other hand, for quadratic function fields, there are recent works [1,3,7] on the distribution of class groups of imaginary quadratic function fields in terms of ℓ-torsion subgroups for a given prime ℓ. In particular, [3] settles the Cohen–Lenstra heuristics (or the Friedman–Washington conjecture) for imaginary function fields, and they use equidistribution results due to Katz–Sarnak [12].

In this paper we work on indivisibility of the class numbers of *real* quadratic function fields. We find an explicit expression for a lower bound of the density of real quadratic function fields whose class numbers are not divisible by a given prime ℓ.

Notation

- $\mathbb{F}$: finite field
- $\mathcal{H}_n(\mathbb{F})$: the space of all monic separable polynomials of degree n in $\mathbb{F}[x]$
- $Cl_f(\mathbb{F})$: a class group of a function field $\mathbb{F}[x,y]/(y^2 = f(x))$ for $f \in \mathbb{F}[x]$.

We state the main result of this paper as follows.

Theorem 1.1. *For a family of finite fields with $|\mathbb{F}| \equiv r \pmod{\ell}$, we have the following:*

$$\frac{\left|\{f(x) \in \mathcal{H}_{2g+2}(\mathbb{F}) \,:\, Cl_f(\mathbb{F})[\ell] \cong 1\}\right|}{\left|\mathcal{H}_{2g+2}(\mathbb{F})\right|} > \begin{cases} 1 + \sum_{j=1}^{g} \prod_{i=1}^{j} \frac{1}{1-\ell^i} - \frac{2(2g+1)!\ell^{g^2}(\ell-1)\prod_{j=1}^{g}(\ell^{2j}-1)}{\sqrt{|\mathbb{F}|}} & \text{if } r \not\equiv 1 \pmod{\ell}, \\ 1 + \sum_{j=1}^{g} \prod_{i=1}^{j} \frac{\ell}{1-\ell^{2i}} - \frac{2(2g+1)!\ell^{g^2}(\ell-1)\prod_{j=1}^{g}(\ell^{2j}-1)}{\sqrt{|\mathbb{F}|}} & \text{if } r \equiv 1 \pmod{\ell}. \end{cases}$$

We therefore obtain the asymptotic lower bound as follows:

$$\lim_{|\mathbb{F}| \equiv r \pmod{\ell},\ |\mathbb{F}| \to \infty} \frac{|\{f(x) \in \mathcal{H}_{2g+2}(\mathbb{F}) \,:\, Cl_f(\mathbb{F})[\ell] \cong 1\}|}{|\mathcal{H}_{2g+2}(\mathbb{F})|} > \frac{\ell-2}{\ell-1}.$$

That is, the proportion of real quadratic function fields whose class number are not divisible by ℓ is greater than $\frac{\ell-2}{\ell-1}$.

We point out that the explicit lower bound of such a density we found only depends on the prime ℓ, the degrees of the discriminants of real quadratic function fields, and the condition: either $r \equiv 1 \pmod{l}$ or not. (It is independent of the value r as long as either $r \equiv 1 \pmod{l}$ or not.)

2. Preliminaries

We introduce some notation which will be used throughout this paper. We use similar notation to that of [1,3].

Notation

- $\mathcal{C}_f$: hyperelliptic curve given by $y^2 = f(x)$ for $f \in \mathbb{F}[x]$
- $Jac(\mathcal{C}_f)(\mathbb{F})$: Jacobian of C_f over $\mathbb{F}$
- $Jac(\mathcal{C}_f)(\mathbb{F})[\ell]$: $\mathbb{F}$ rational ℓ-torsion subgroup of $Jac(\mathcal{C}_f)$
- $GSp_{2g}(\mathbb{Z}/\ell) = \{A \in GL(V) \,|\, \exists m(A) \in (\mathbb{Z}/\ell)^\times : \forall v, w \in V, \langle Av, Aw\rangle = m(A)\langle v, w\rangle\}$, where V is a free $\mathbb{Z}/\ell$-module of rank $2g$, for an odd integer ℓ, a natural integer g